Managing SSL server certificates

Use the **Security → SSL Server Certificates** screen to establish and maintain the certificates presented for access to the PingFederate administrative console (or the administrative API) and for incoming HTTPS connections at runtime.

The first system-generated certificate is the default certificate for both the administrative console and the runtime server. As multiple certificates are created, they can be activated (or deactivated) for the administrative console, the runtime server, or both. Additionally, any of them may be selected as the new default certificate for the administrative console, the runtime server, or both at a latter time.

When creating a certificate, additional domain names may be added through the use of the **Subject Alternative Names** field. Furthermore, if a user agent includes the host name that it intends to reach as part of the TLS handshake, PingFederate selects the applicable certificate based on the provided SNI (Server Name Indication) information. The selection looks at the common name and subject alternative names of each activated certificate. If PingFederate finds no match, it serves the default certificate. If PingFederate finds multiple matches, it serves the certificate with the better match. Consider the following sample configuration and inbound requests.

SSL Server Certificates configuration

Certificate	Common name	Subject alternative names	Activation status
#1	`www.example.com`	(None)	Administrative console and runtime server
#2	`www.example.org`	`*.example.org` and `test.example.local`	Administrative console and runtime server
#3	`www.example.info`	`*.example.info` and `*.example.com`	Administrative console and runtime server
#4	`admin.example.local`	(None)	Administrative console (Default) and runtime server
#5	`runtime.example.local`	(None)	Administrative console and runtime server (Default)

Runtime behavior

Request type	Host name from SNI	Certificate served
Administrative or runtime	www.example.com	The host name from the SNI is an exact match to the common name of certificate #1 and a partial match to the second subject alternative name (`*.example.org`) of certificate #3.

Request type	Host name from SNI	Certificate served
		An exact match is a better match; therefore, PingFederate serves certificate #1.
Administrative or runtime	www.example.org	The host name from the SNI is an exact match to the common name of certificate #2. PingFederate serves certificate #2.
Administrative or runtime	sso.example.org	The host name from the SNI is a partial match to the first subject alternative name (`*.example.org`) of certificate #2. There is no other exact or partial match. PingFederate serves certificate #2.
Administrative or runtime	sso.example.info	The host name from the SNI is a partial match to the first subject alternative name (`*.example.info`) of certificate #3. There is no other exact or partial match. PingFederate serves certificate #3.
Administrative or runtime	sso.example.com	The host name from the SNI is a partial match to the second subject alternative names (`*.example.com`) of certificate #3. There is no other exact or partial match. PingFederate serves certificate #3.
Administrative	www.example.local	The host name from the SNI does not match any configured certificate. PingFederate serves certificate #4, the default certificate for the administrative console.
Runtime	localhost	The host name from the SNI does not match any configured certificate. PingFederate serves certificate #5, the default certificate for the runtime server.

Note:

If PingFederate finds multiple certificates of the same matching quality, it returns one of them in the TLS handshake. This response should not impact the user agent because either the common name or one of the subject alternative names matches the host name of the request. If PingFederate should always serve a particular certificate for any given host name, ensure that the common name and any configured subject alternative names do not overlap among multiple certificates.

Creating a new certificate

1. On the **SSL Server Certificates** screen, click **Create new**.

2. On the Create Certificate screen, enter the required information.

   For information about each field, refer to the following table:

Field	Description
Common Name	The common name (CN) identifying the certificate.
Subject Alternative Names	The additional DNS names or IP addresses that can be associated with the certificate.
Organization	The organization (O) or company name creating the certificate.
Organizational Unit	The specific unit within the organization (OU).
City	The city or other primary location (L) where the company operates.
State	The state (ST) or other political unit encompassing the location.
Country	The country (C) where the company is based.
Validity (days)	The time during which the certificate is valid.
Cryptographic Provider	The storage facility of the certificate. Applicable and visible only when PingFederate is integrated with an HSM in hybrid mode. • Select HSM to store the certificate in the HSM. • Select Local Trust Store to store the certificate in the local trust store managed by PingFederate.
Key Algorithm	A cryptographic formula used to generate a key. PingFederate uses either of two algorithms, RSA or EC.
Key Size (bits)	The number of bits used in the key. (RSA-1024, 2048 and 4096; and EC-256, 384 and 521.)
Signature Algorithm	The signing algorithm of the certificate. (RSA-SHA256, SHA384, and SHA512; and ECDSA-SHA256, SHA384, and SHA512.)

3. When finished, click **Next**.
4. On the **Summary** screen, review your configuration, amend as needed, and click **Save**.

Importing a certificate and its private key

1. On the **SSL Server Certificates** screen, click **Import**.
2. On the **Import Certificate** screen, choose the applicable certificate file and enter its password.

   Note:

   If PingFederate is integrated with an HSM from Thales, it is not possible to use an elliptic curve (EC) certificate as an SSL server certificate. You must select a certificate that uses the RSA key algorithm.

If PingFederate is integrated with an HSM in hybrid mode, select the storage facility of the certificate from the **Cryptographic Provider** list.

- Select **HSM** to store the certificate in the HSM.
- Select **Local Trust Store** to store the certificate in the local trust store managed by PingFederate.

3. On the **Summary** screen, review your configuration, amend as needed, and click **Save**.

Creating a certificate-authority signing request (CSR)

1. On the **SSL Server Certificates** screen, select **Certificate Signing** under **Action** for the certificate.

   Note:

   This selection is inactive if you have not yet saved a newly created or imported certificate. Click **Save** and then return to this screen to initiate the process.

   The selection is also inactive if a previously signed certificate has been revoked. Because the revocation may indicate that the private key has been compromised, the best practice is to import or create a replacement certificate for certificate signing.

2. On the **Certificate Signing** screen, select the **Generate CSR** option.
3. On the **Generate CSR** screen, click **Export** to save the CSR file, and then click **Done**.

   Once saved, you can submit this CSR file to a certificate authority (CA) for a CA-signed certificate.

Importing a certificate-authority response (CSR response)

1. On the **SSL Server Certificates** screen, select **Certificate Signing** under **Action** for the certificate.
2. On the **Certificate Signing** screen, select the **Import CSR Response** option.
3. On the **Import CSR Response** screen, choose the applicable CSR response file.
4. On the **Summary** screen, review your configuration, and click **Save**.

Exporting a certificate

1. On the **SSL Server Certificates** screen, select **Export** under **Action** for the certificate.
2. On the **Export Certificate** screen, select the export type.

- Select **Certificate Only** to export the selected certificate without its private key. This is the default choice.
- Select **Certificate and Private Key** to export the selected certificate with its private key.

CAUTION:

This export contains the private key of the certificate. You must also enter an encryption password.

If the selected certificate is stored in an HSM, the **Certificate and Private Key** option does not apply.

3. On the **Export & Summary** screen, click **Export** to save the certificate file, and then click **Done**.

Reviewing a certificate

1. On the **SSL Server Certificates** screen, select the certificate by its serial number.
2. Review the selected certificate in the pop-up window.

   When finished, close the pop-up window.

Activating or deactivating a certificate

1. On the **SSL Server Certificates** screen, select the relevant option under **Action** for the certificate.

   Any certificate can be activated for the administrative console, the runtime server, or both.

   When multiple certificates are activated for the administrative console (or the runtime server), you can deactivate any of them as long as one certificate remains active. Additionally, you may select any of them as the default certificate.

2. Click **Save** to keep your configuration.

Removing a certificate

1. On the **SSL Server Certificates** screen, select **Delete** under **Action** for the certificate.

If the selected certificate is activated for the administrative port, the runtime port, or both, the **Delete** option does not apply.

To cancel the removal request, select **Undelete** under **Action** for the certificate.

2. Click **Save** to confirm your action.